Exceptional service in the national interest

Sandia National Laboratories

DNSViz - Monitoring, Analysis, and Visualization

Casey Deccio

Sandia National Laboratories

DNS-OARC Fall 2013 Workshop, Phoenix, AZ

October 5, 2013

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

From textual command line…

Sandia National Laboratories

sandia.gov/DS

```
$ dig +dnssec +noall +answer @a.gov-servers.net sandia.gov ds
sandia.gov.          86400  IN    DS     20739 7 1 3CA461FF5496BC72A772056489D944621EDA774E
sandia.gov.          86400  IN    DS     20739 7 2 0C5F4CDFF8824665ACD1D8A132951B193C59FA7FE6CF7B1F82484C25
B410CDC6
sandia.gov.          86400  IN    DS     36033 7 1 E33B4526CECF2A1B7C733D645B30CD5C912D9538
sandia.gov.          86400  IN    DS     36033 7 2 4677626ABE69FD1D8DD8E5DE10533D2B264A91A7BF1AB3A6BFFC4C40
8A3752FF
sandia.gov.          86400  IN    RRSIG  DS 7 2 86400 20130423160022 20130418160022 32416 gov. AJ1D8NdBoz…
```

sandia.gov/DNSKEY

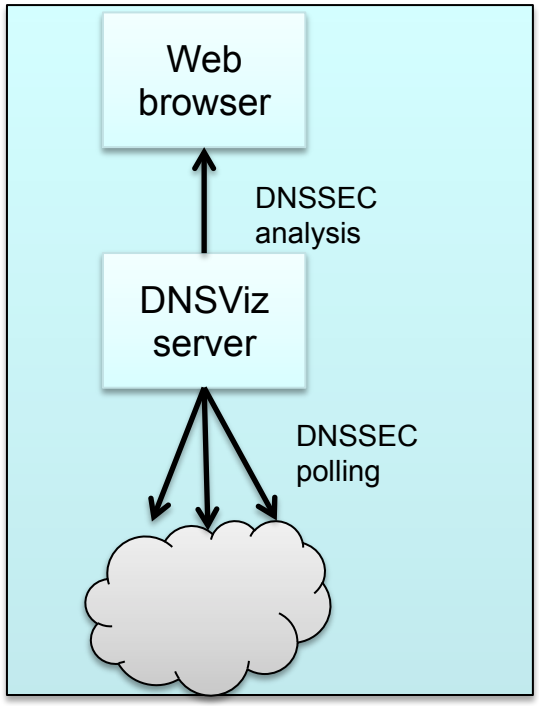
```
$ dig +dnssec +noall +answer @ns1.ca.sandia.gov sandia.gov dnskey
sandia.gov.          3600   IN    DNSKEY     257 3 7 AwEAAb80HH…
sandia.gov.          3600   IN    DNSKEY     257 3 7 AwEAAeWCW…
sandia.gov.          3600   IN    DNSKEY     256 3 7 AwEAAb0B0c…
sandia.gov.          3600   IN    DNSKEY     256 3 7 AwEAActQCC…
sandia.gov.          3600   IN    RRSIG  DNSKEY 7 2 3600 20130507100332 20130407100332 20739 sandia.gov. NvFqboaPz…
sandia.gov.          3600   IN    RRSIG  DNSKEY 7 2 3600 20130507100332 20130407100332 36033 sandia.gov. c+f2sq8OE7…
sandia.gov.          3600   IN    RRSIG  DNSKEY 7 2 3600 20130507100332 20130407100332 47459 sandia.gov. VMBjLv/M3…
```

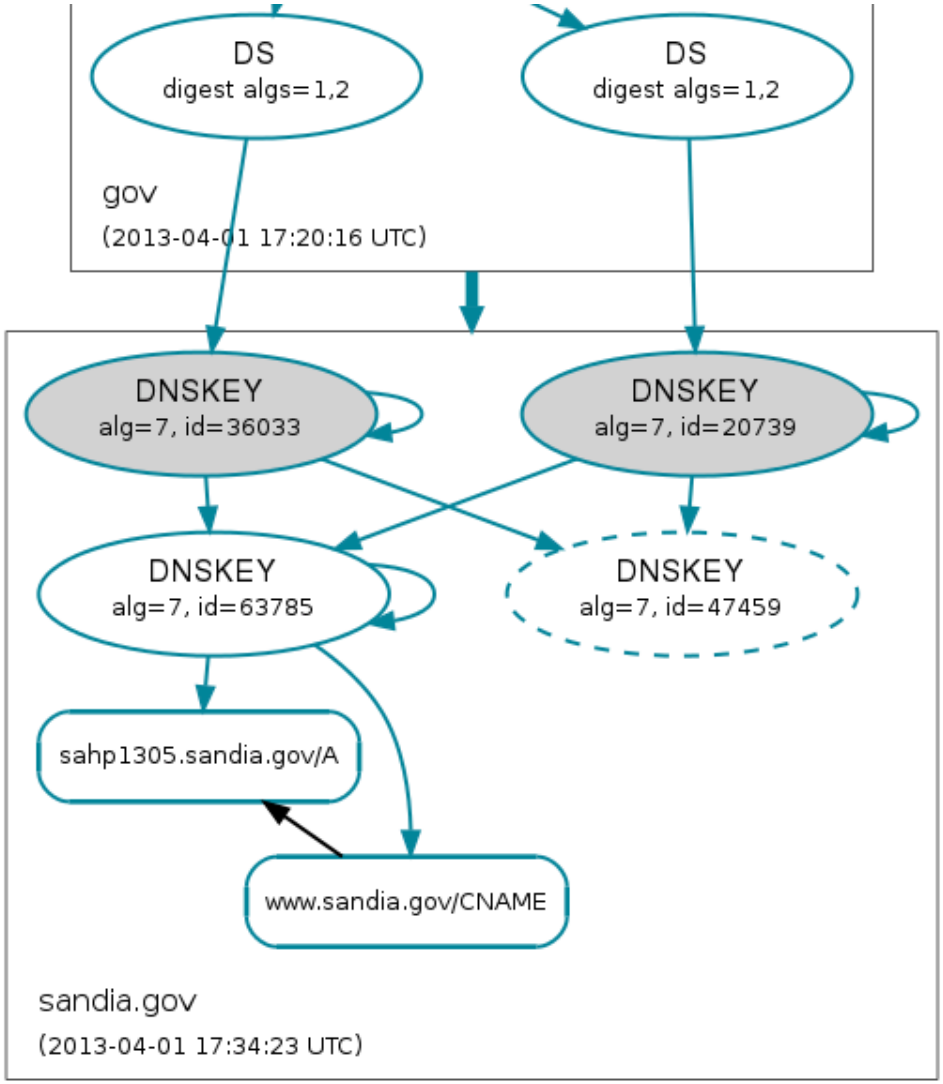
www.sandia.gov/A

```
$ dig +dnssec +noall +answer @ns1.ca.sandia.gov www.sandia.gov a
www.sandia.gov.              3600   IN    CNAME      sahp1305.sandia.gov.
www.sandia.gov.              3600   IN    RRSIG  CNAME 7 3 3600 20130507100332 20130407100332 47459 sandia.gov. qaIx62vES…
sahp1305.sandia.gov.         3600   IN    A      132.175.81.4
sahp1305.sandia.gov.         3600   IN    RRSIG  A 7 3 3600 20130507100332 20130407100332 47459 sandia.gov. Qzy5HlXxd…
```

…to graphical Web browser

- DNSViz polls all servers necessary to analyze a DNS domain
- Consolidates data into graphical Web interface: http://dnsviz.net/

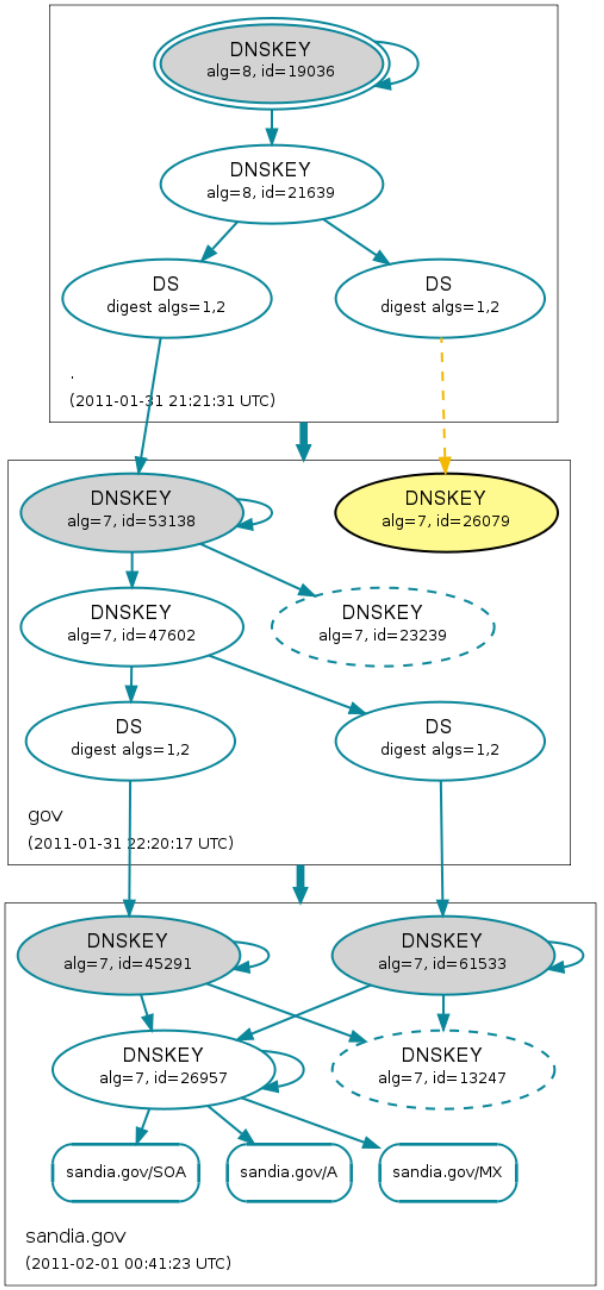




DNSSEC validation status

- **Secure** – unbroken chain from anchor to RRset

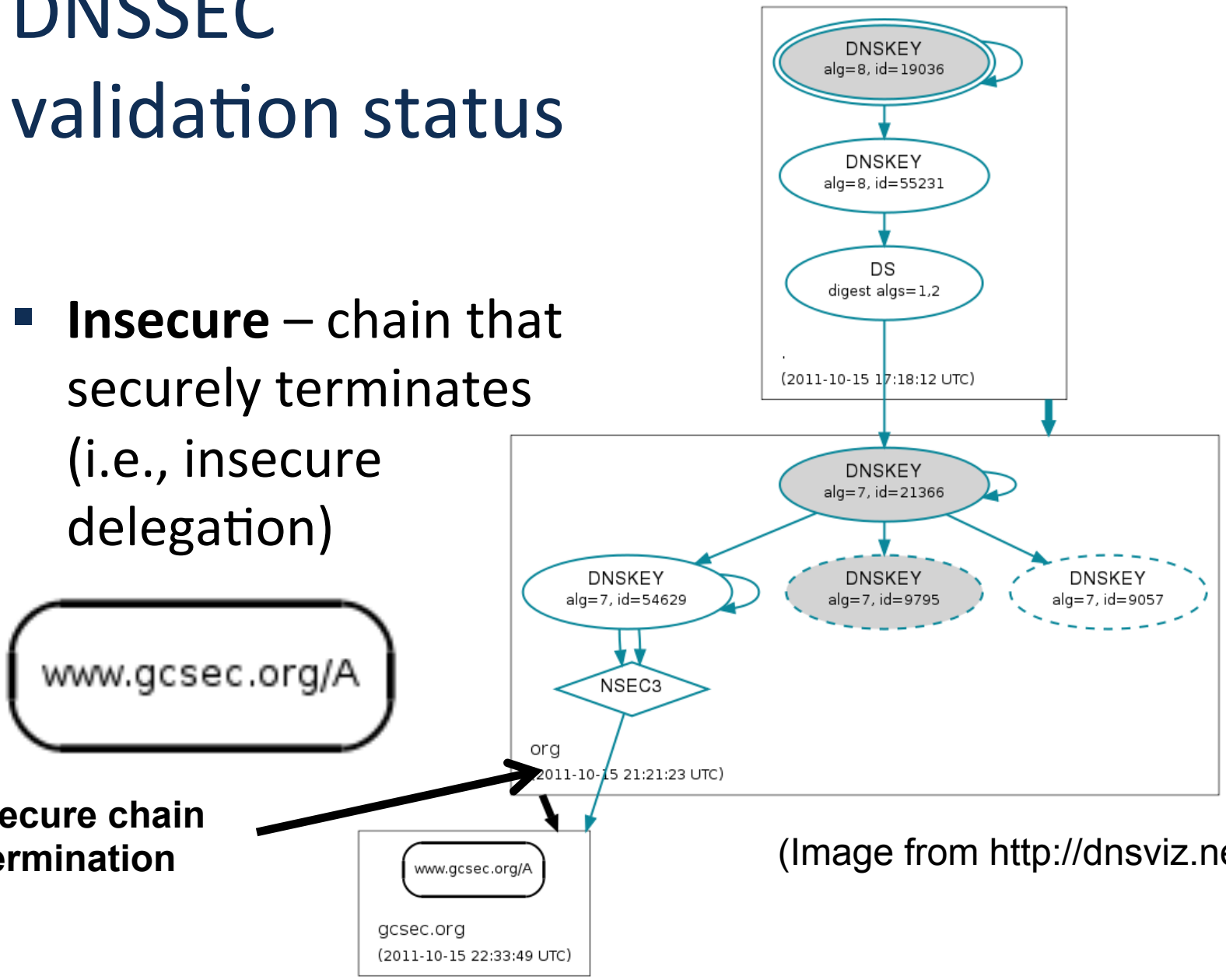
sandia.gov/SOA



(Image from http://dnsviz.net/)

DNSSEC validation status

- **Insecure** – chain that securely terminates (i.e., insecure delegation)



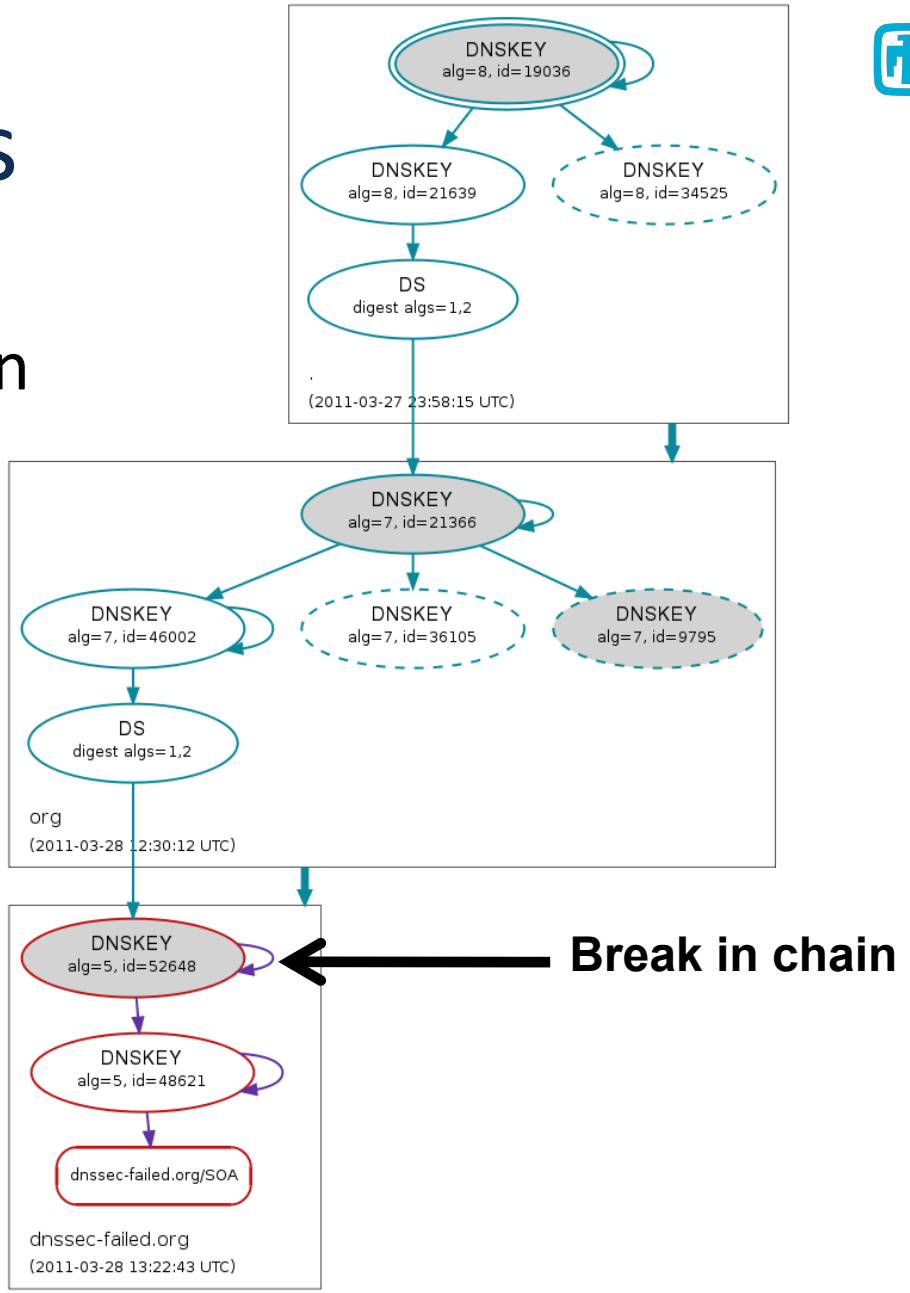
Secure chain termination

(Image from http://dnsviz.net/)

DNSSEC validation status

- **Bogus** – broken chain

dnssec-failed.org/SOA

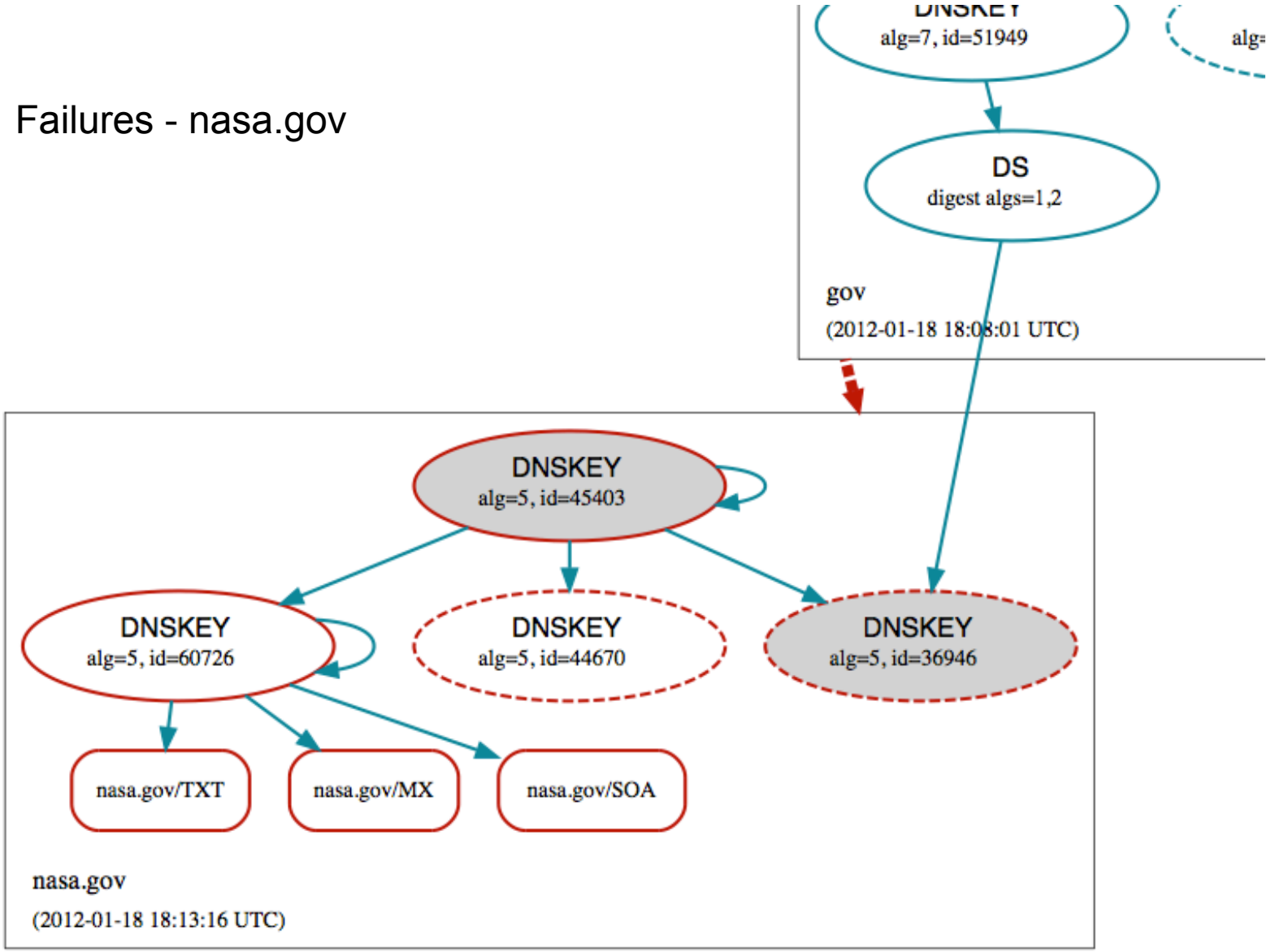


Break in chain

(Image from http://dnsviz.net/)

Sandia National Laboratories

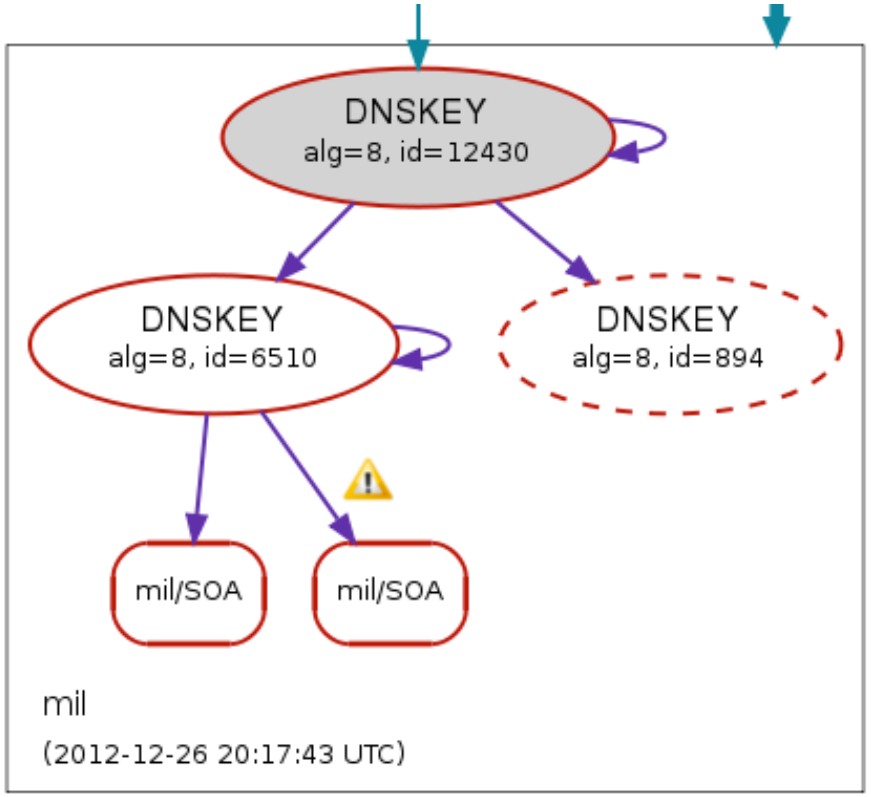
Failures - nasa.gov



http://dnsviz.net/d/nasa.gov/TxcLvQ/dnssec/

Sandia National Laboratories

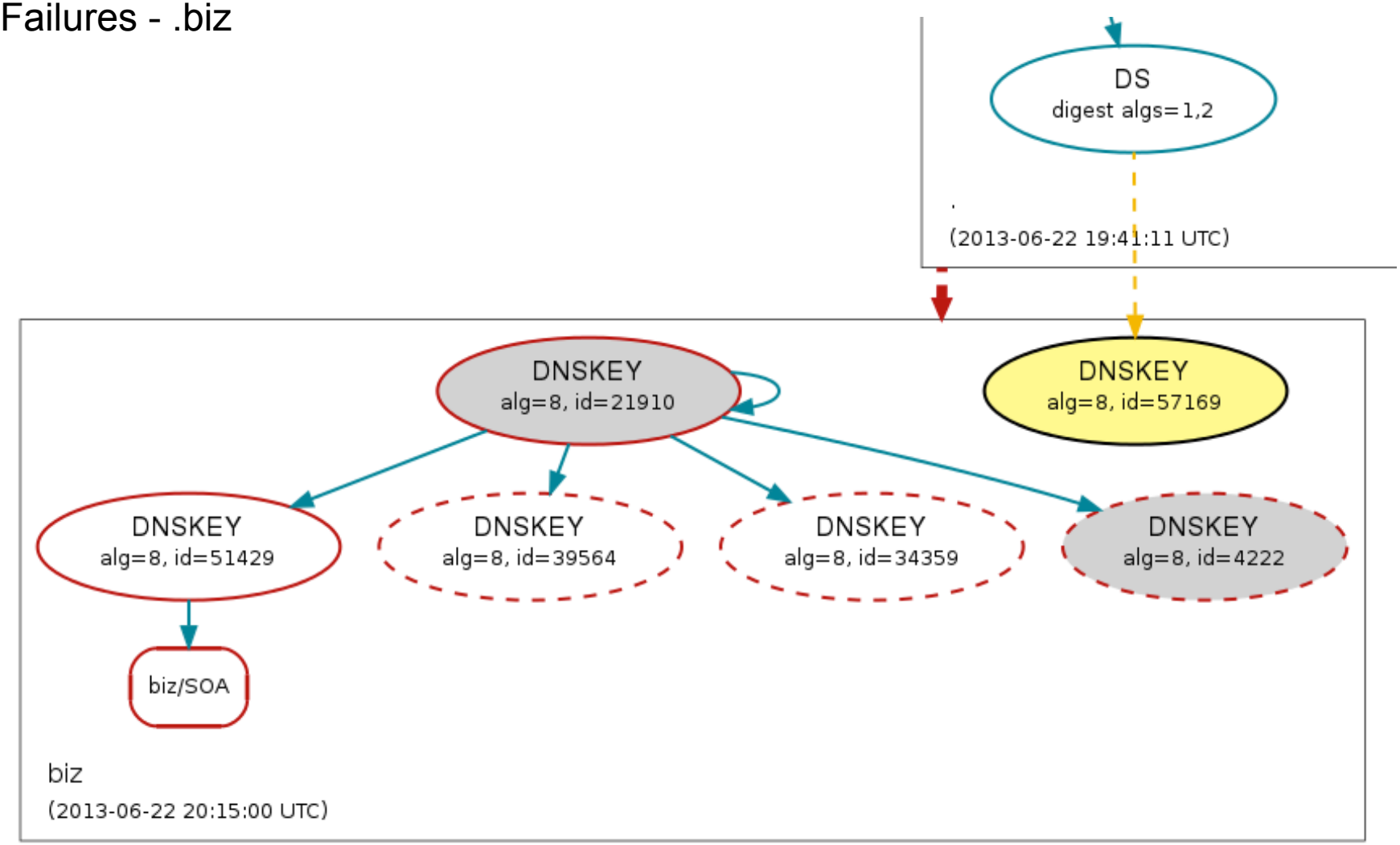
Failures - .mil



http://dnsviz.net/d/mil/UNwzNg/dnssec/

Sandia National Laboratories

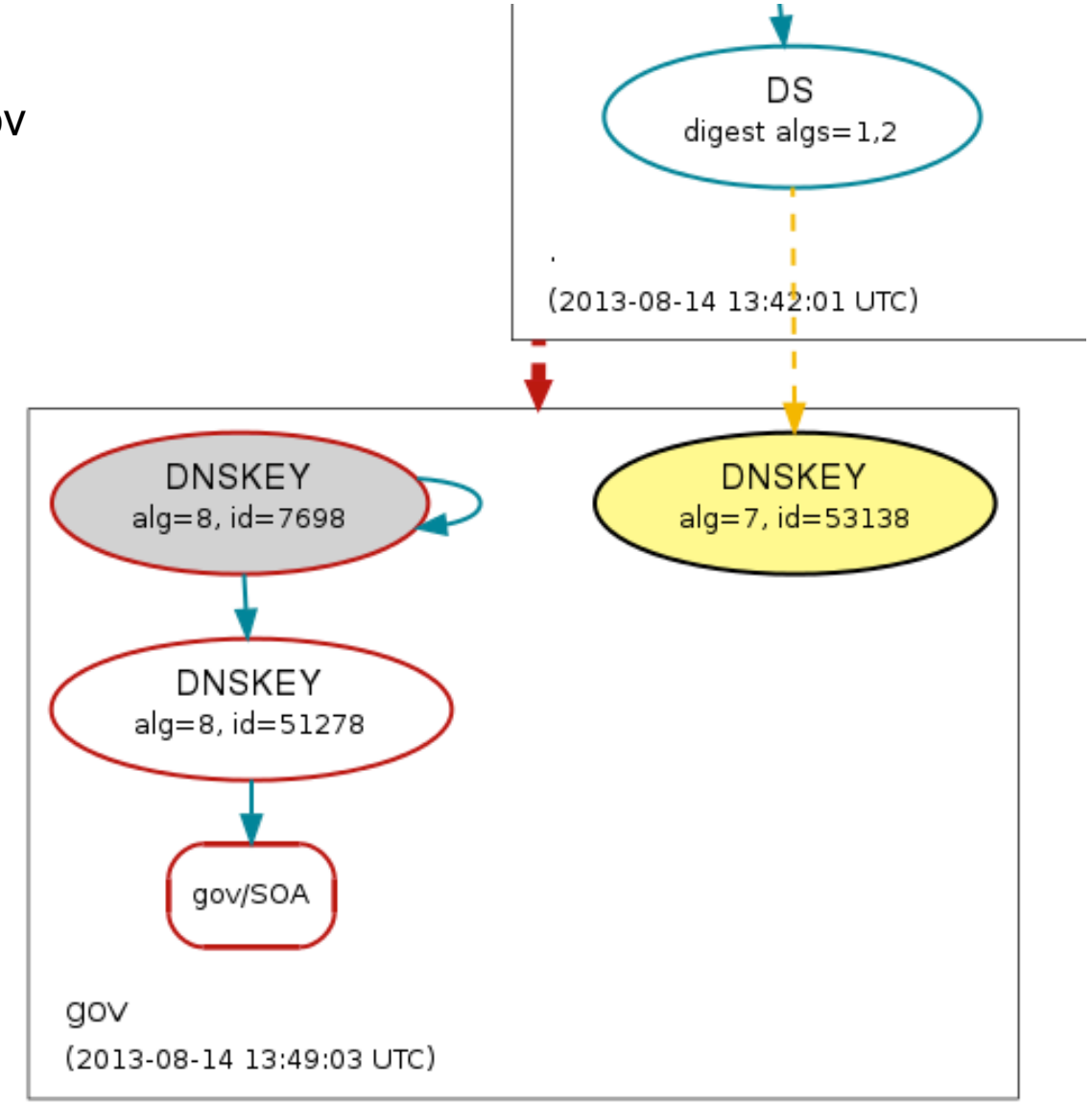
Failures - .biz



http://dnsviz.net/d/biz/UcYFxQ/dnssec/

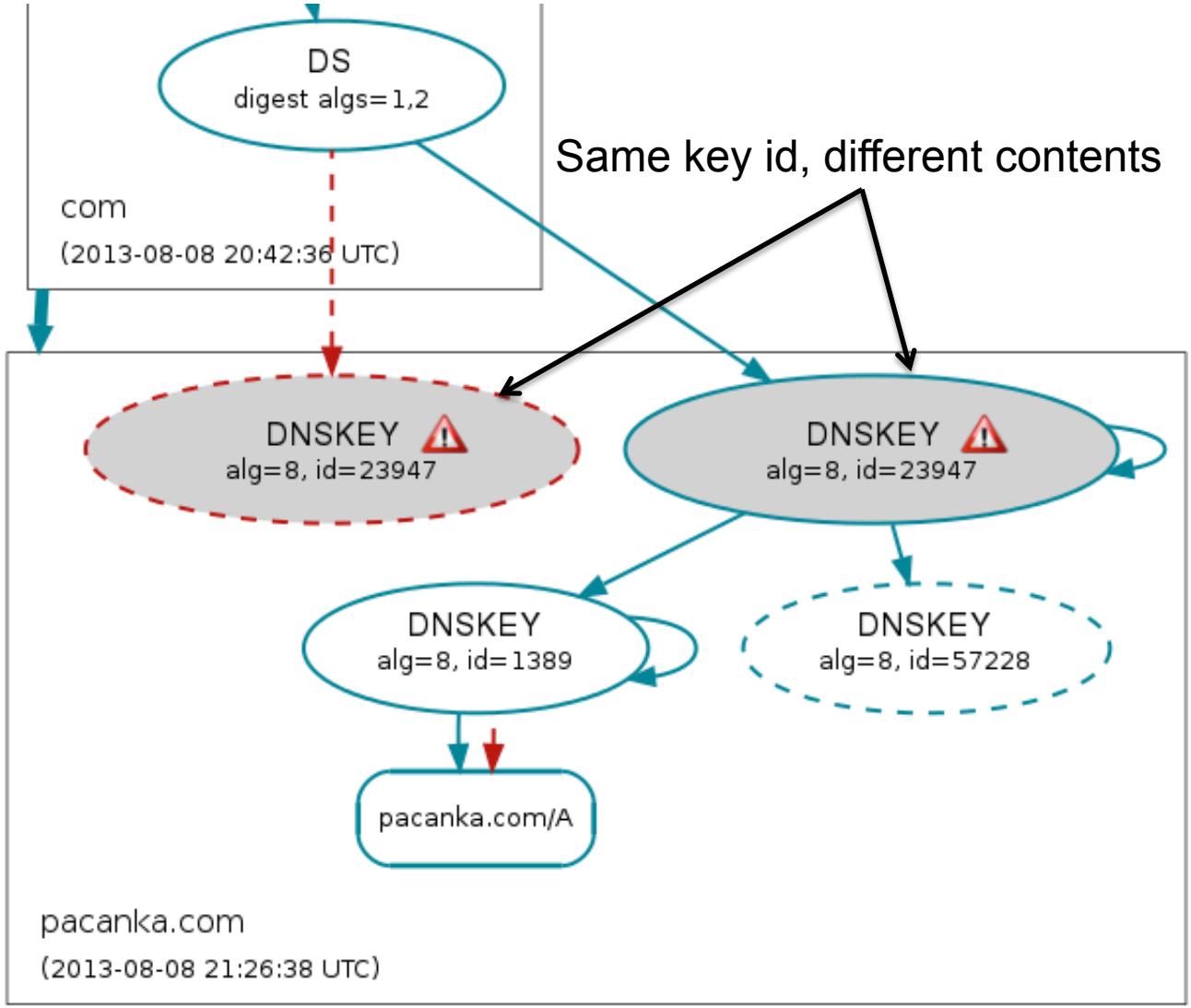
Sandia National Laboratories

Failures - .gov



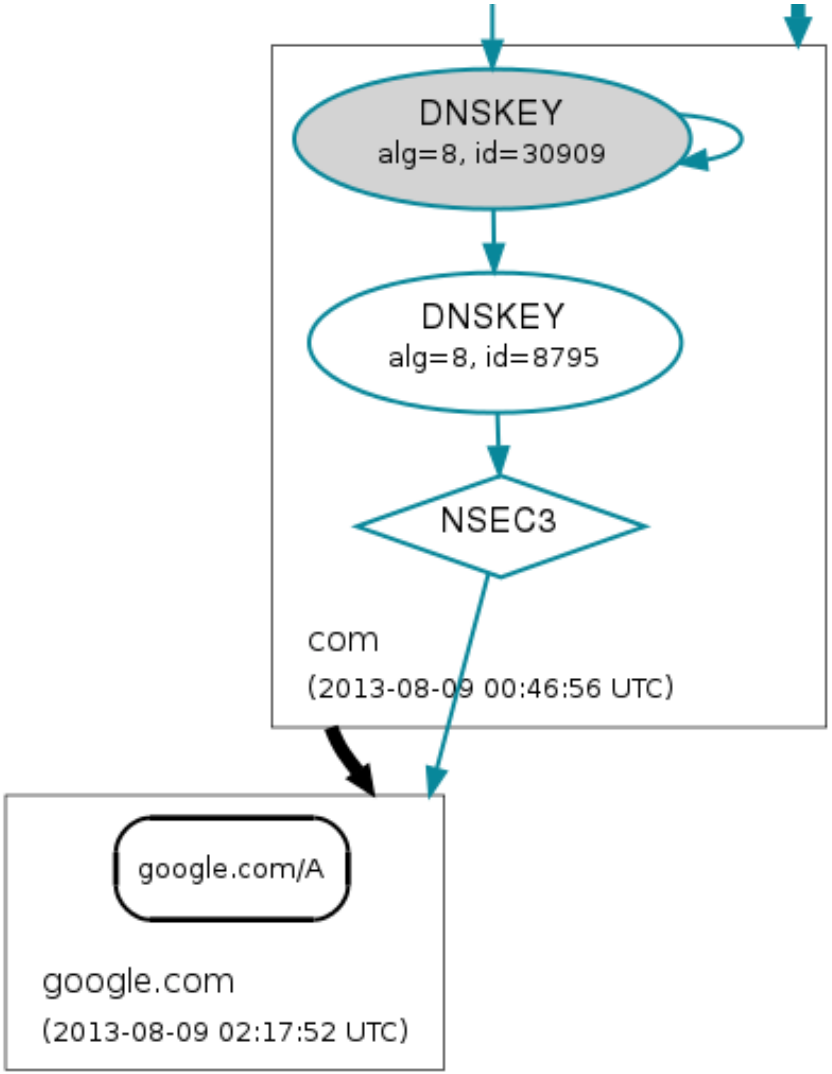
http://dnsviz.net/d/gov/UguK0A/dnssec/

Different Records on Servers

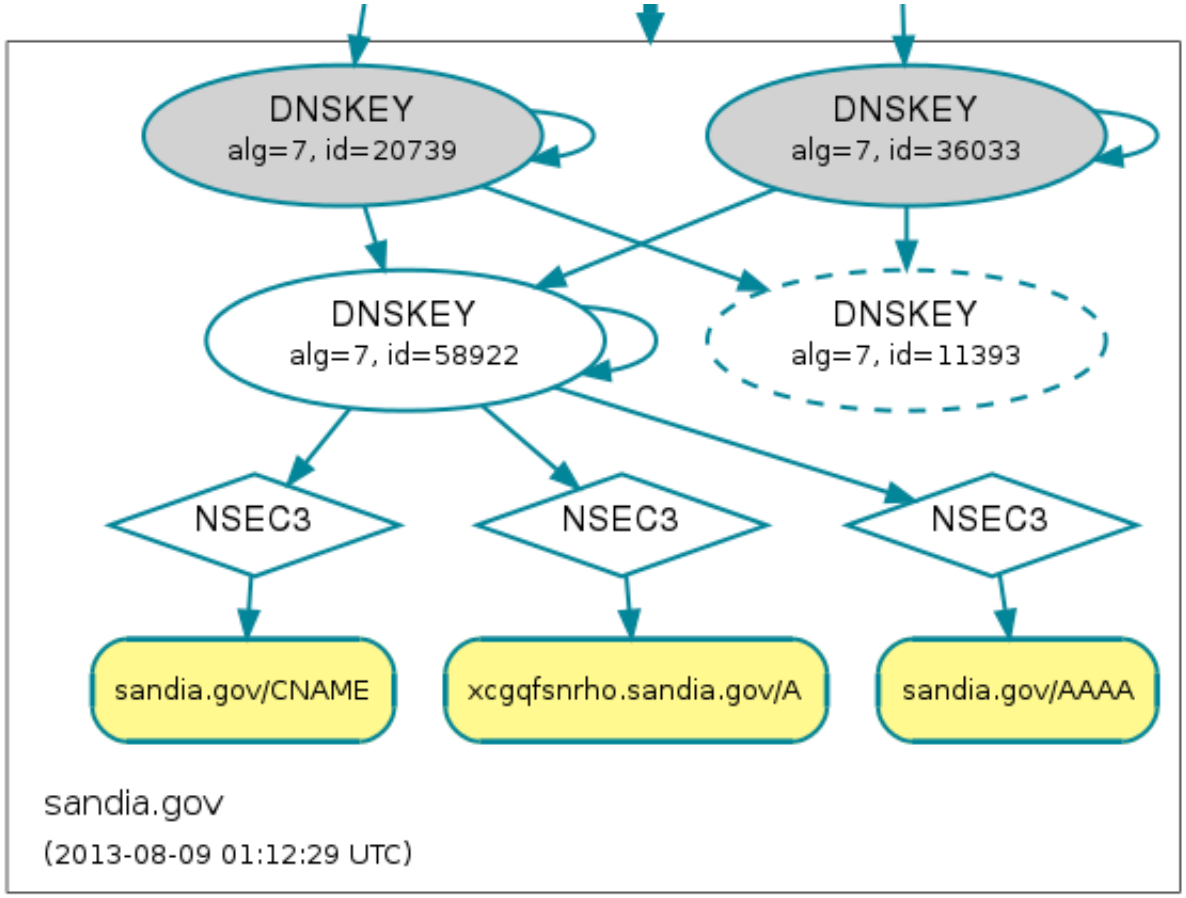


http://dnsviz.net/d/pacanka.com/UgQNDw/dnssec/

NSEC(3) Records – insecure delegation

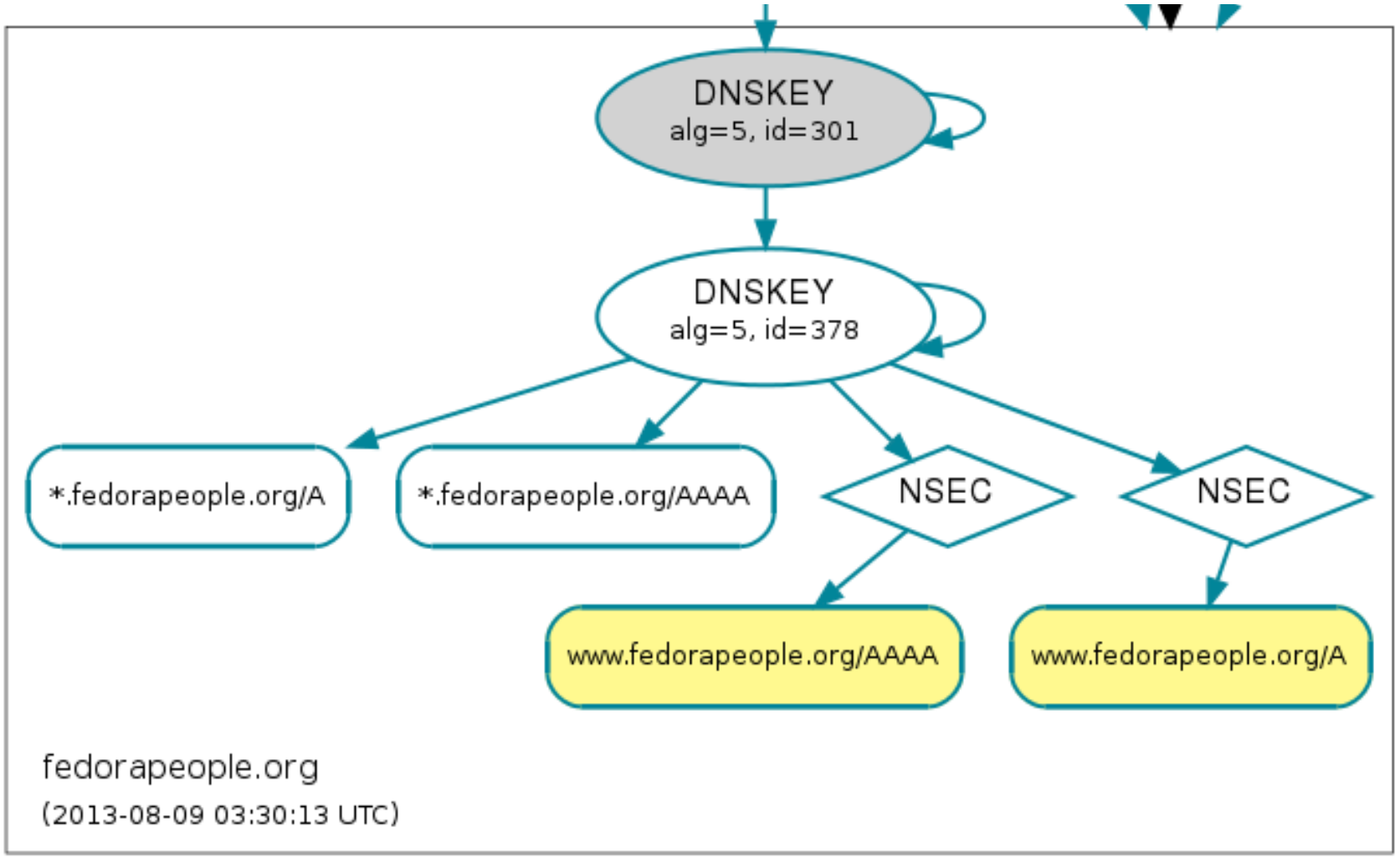


NSEC(3) Records – Other denial of existence

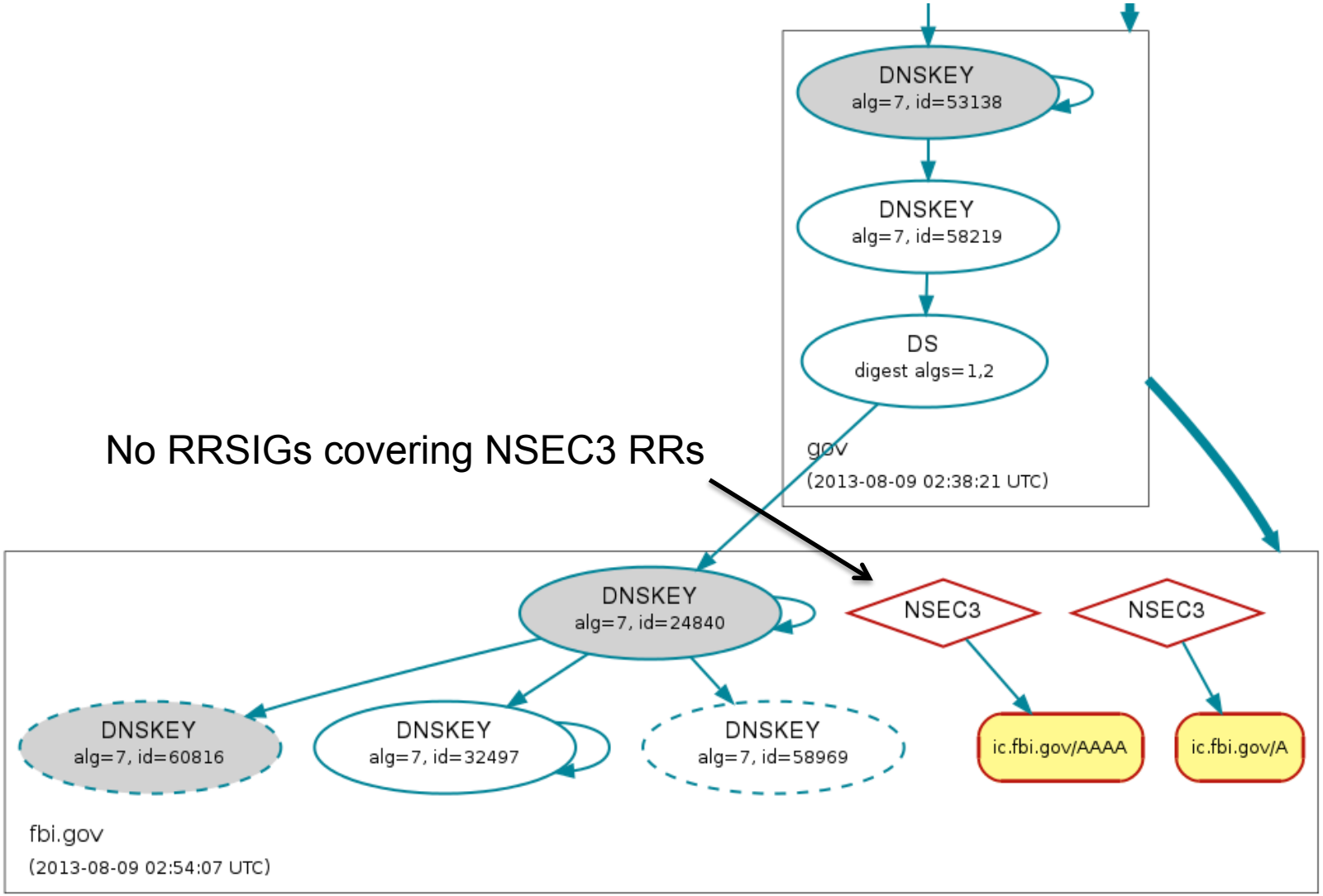


NSEC(3) Records - Wildcards

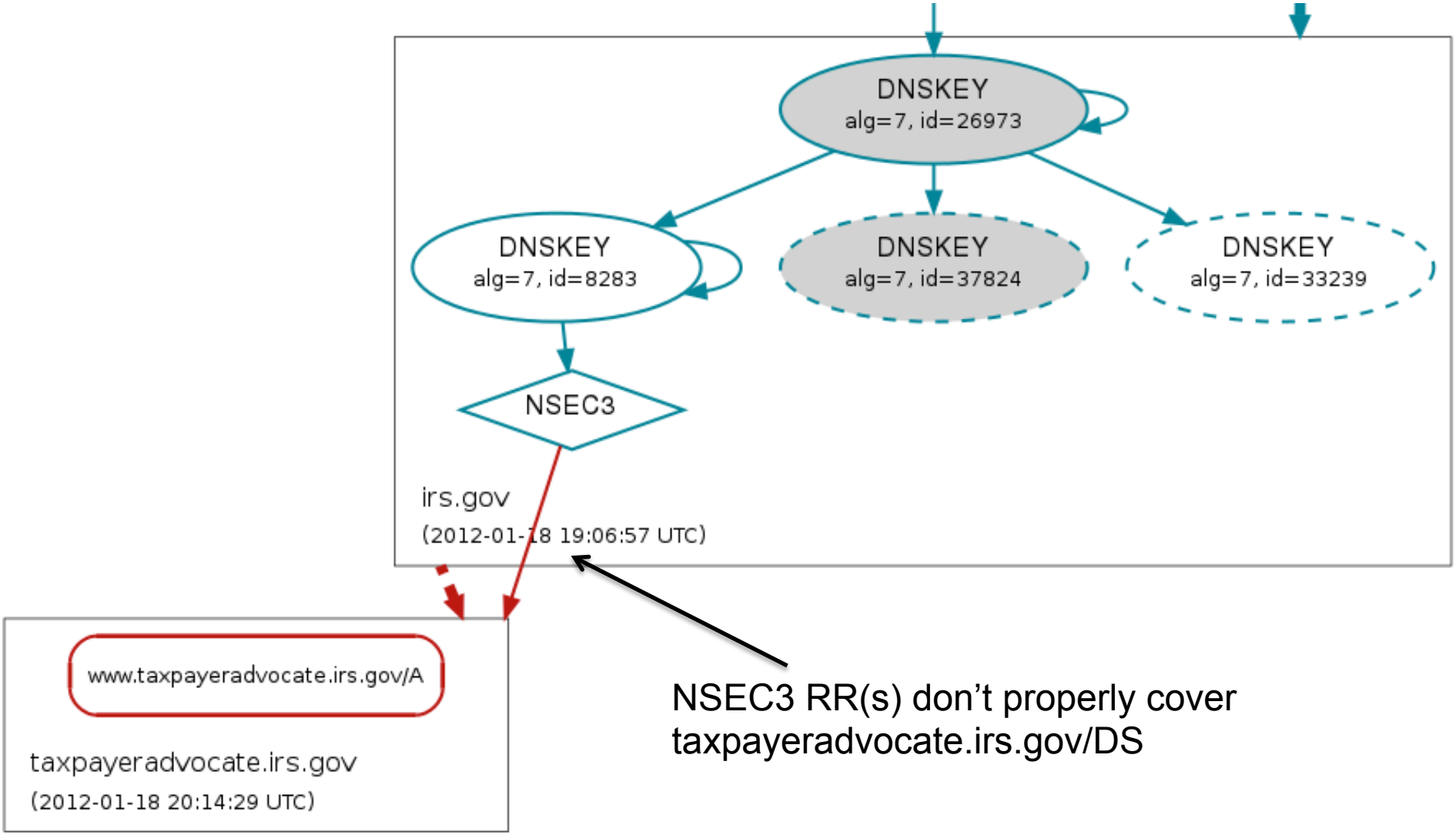
Sandia National Laboratories



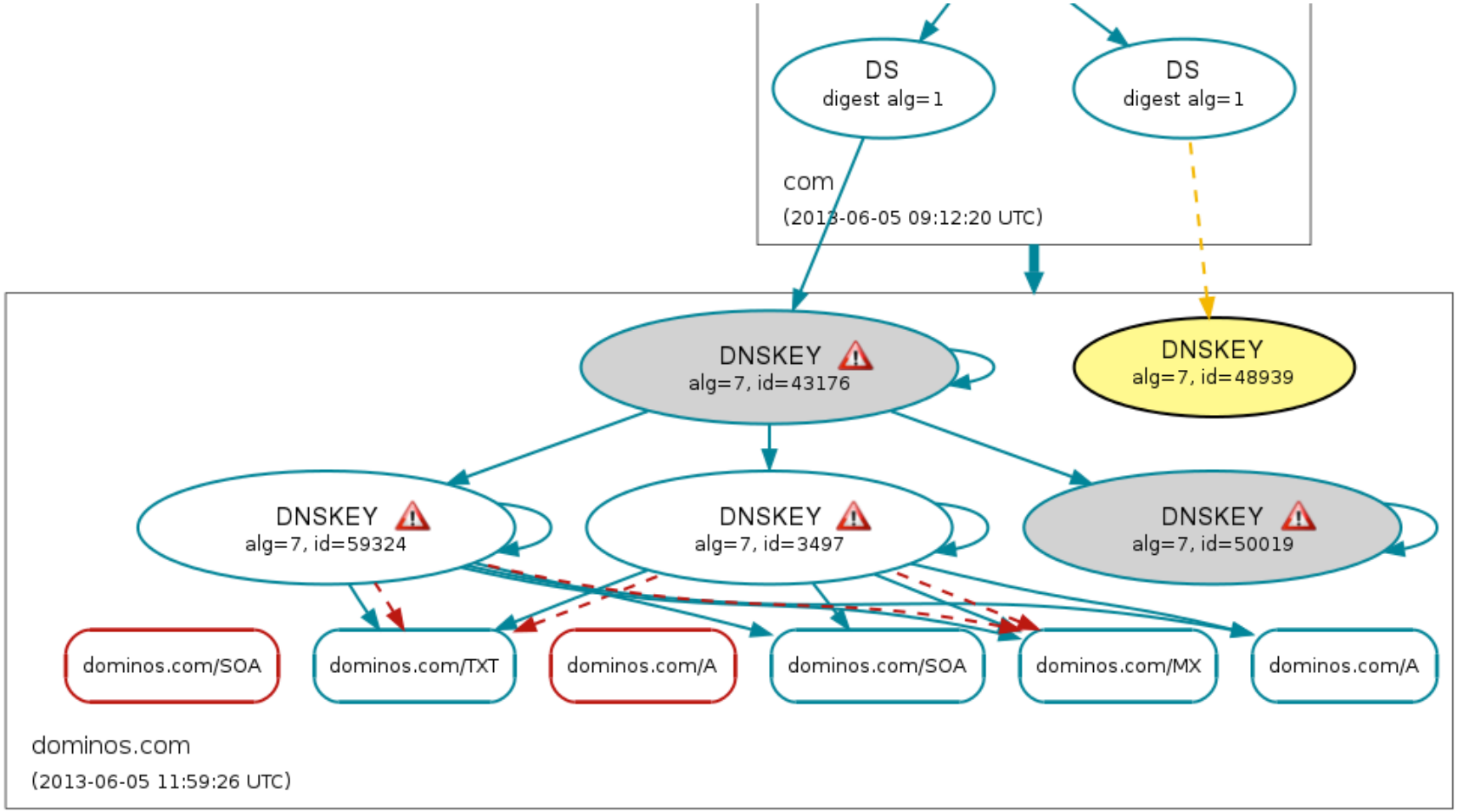
NSEC(3) Records and RRSIGs



NSEC(3) Failures



Multiple Paths



DNSViz Features – Current

Sandia National Laboratories

- DNSSEC authentication
  - Chain of trust visualization
  - Misconfiguration identification
- Authoritative server response
  - TCP/UDP responsiveness
  - EDNS, DNSSEC, NSEC(3)
  - PMTU issues
  - Delegation correctness/consistency
  - Response consistency
- Historical analysis

DNSViz Features – Planned

Sandia National Laboratories

- Full dependency analysis
  - NS, MX, CNAME dependencies
- Real-time "at-a-glance" analysis
- API
  - RESTful Web API
  - Structural analysis representation
  - Integration with other tools/databases
- Perspectives
  - Analysis looking glasses – different vantage points
  - Cache introspection
    - From server perspective
    - From client perspective
  - Passive feeds
- Subscriptions
  - Email notification
  - Feeds
- Other
  - Performance optimization
  - Various bug fixes, usability requests

DNSViz – Architecture

Sandia National Laboratories

- Database History
  - 1st Generation – PostgreSQL
    - No history – snapshot only
    - Storage of meta information
  - 2nd Generation – Cassandra
    - History
    - Full response storage
  - 3rd Generation – PostgreSQL
    - History, including migrated cassandra history
    - Full response storage
    - Index of response rdata, including DNSKEYs
- Current status
  - Combination 2nd and 3rd generation code and data, partially migrated

Hosting, Development, and Involvement

Sandia National Laboratories

- Hosting
  - Primary
    - Web services
    - Database
    - DNS polling and analysis
  - Secondary
    - Distributed analysis looking glasses
- Development, discussion, and direction
  - Features, priority, usefulness, etc.
  - Development
  - Integration into other tools
- Involvement
  - How can involvement make this a more useful tool for the DNS community?